

CROWDFUNDING

1. Are crowdfunding websites required to report suspicious transactions?

Crowdfunding websites are not designated as reporting entities that are required to report financial transactions to FINTRAC. With that said, crowdfunding platforms typically employ third-party payment processors to provide the backend infrastructure for the completion of payments involved in a crowdfunding campaign.

A payment service provider may be subject to the obligations and requirements outlined in the PCMLTFA and its associated Regulations if it meets the definition of one of the reporting entity sectors such as an MSB, FMSB, or possibly a financial entity.

2. Would FINTRAC be able to observe the presence of foreign funding in crowdfunding campaigns in Canada?

As per the PCMLTFA, FINTRAC has the authority to receive financial transaction reporting related to cash or electronic transactions that are over CA\$10,000 in value and where the party/parties to the transaction (and the related transfer instructions) indicate that the funds in question are not contained within Canadian borders. As a result, international wire transfers used for crowdfunding donations/contributions by individuals that are valued at CA\$10,000 or more are visible to FINTRAC under Canada's current legislative framework.

There are limits to what a Canadian reporting entity (RE) may be able to see with respect to a crowdfunding-related transaction. In instances where a crowdfunding platform has a payment receipt and disbursement arrangement with a payment processor, the Canadian reporting entity will likely only observe transactions where the payment processor and the crowdfunding platform are the ordering and beneficiary clients. This means that the identity of individual donors is unlikely to be known to a reporting entity. This, of course, depends on the payment and disbursement arrangements of the parties involved. In those instances where the crowdfunding platform undertakes disbursements directly, it would be possible for the reporting entity to identify the beneficiary client (probably the crowdfunding project owner).

3. What are possible red flags of higher risk activity associated with crowdfunding?

- Individuals who sends funds to crowdfunded projects that relate to controversial projects that promote a partisan perspective on an ongoing armed conflict that also involves one or more listed terrorist entities;
- Crowdfunded projects through platforms that have weak project review policies and/or have terms of service that do not specifically exclude causes linked to material support for parties engaged in, or supportive of extremist violence or armed conflict
- Transactions to/through a crowdfunding platform that uses a third party payment processor which the reporting entity (RE) believes has weak or unsatisfactory customer due diligence (CDD) policies and/or weak anti-money laundering (AML) / counter terrorist financing (CTF) controls (e.g. adverse

industry news related to the payment processor, media reporting discussing exploitation of payment processor by illicit financial actors, etc.);

- Transactions to suspicious crowdfunded projects, where the donor / pledger appears to use excessive security controls and/or measures to obscure their identity or the source of funds when this would be unnecessary or uncommon for many other crowdfunded projects;
- Transactions of individual donors executed by a third party payment processor, cannot reliably be associated with an unmasked internet protocol (IP) address (meaning the user has used security tradecraft to obscure their IP address);
- Relevant adverse information is discovered related to the promoters or backers of crowdfunding projects that suggests a past history of hate speech, glorification / promotion of listed terrorist entities, facilitation of terrorist activity, or incitement to violence or participation in terrorist acts or terrorist organizations; and,

4. What has FINTRAC observed in relation to crowdfunding specifically by IMVE threat actors?

FINTRAC has observed a number of key patterns in IMVE threat actors when analyzing reporting that contained a reference to IMVE-related activity. For cross-border networks, FINTRAC has noted that individuals in Canada that may fund international IMVE networks, while not necessarily being members of organized groups themselves typically used payment processing companies and money services businesses to make international funds transfers. In instances wherein organized groups used personal accounts, FINTRAC observed several IMVE-related payments to personal accounts from crowdfunding sites. Since the addition of multiple IMVE threat actors to Canada's list of terrorist entities, FINTRAC has observed an increase in the amount of high-quality and relevant STRs submitted relating to IMVE-suspected financing, and continues to produce key strategic intelligence on emerging trends with regard to the use of crowdfunding by IMVE threat actors.

IMVE AND VIRTUAL CURRENCY

5. Have IMVE threat actors solicited donations using virtual currencies?

IMVE threat actors have operated successful campaigns either with or without the help of virtual currency crowdfunding platforms. IMVE threat actors have been known to launch campaigns on social media platforms such as Twitter, reddit, Instagram or youtube in order to publicly post information about their cause and a virtual currency wallet address to send funds to.

In contrast, the use crowdfunding platforms allows these actors to potentially save on transfer fees which could add up to significant amounts if there is a large volume on incoming donations. Crowdfunding platforms also helps in making the entire campaign process more manageable and seamless. The benefits include advertising the campaign, the cause, and cryptocurrency address on crowdfunding website, making the process simple and accessible for donors.

IMVE threat actors that subscribe to xenophobic and racist ideologies such as the Proud Boys, Counter Currents, Free Domain Radio, Weev, Stormfront, Daily Stormer, VDare, American Renaissance have been known to resort to cryptocurrency for funding campaigns once their accounts with banking institutions, platforms such as Patreon and GoFundMe are closed due to suspect activity. Decentralized blockchain

and cryptocurrency allow the actors to raise funds without as much oversight from banking institutions and government. Websites such as Tallycoin are an example of how Virtual currency crowdfunding can also facilitate the donation process, having designated postings on their website for campaigns, making the donation process simple for donators.

6. Has FINTRAC observed IMVE threat actors using virtual currency to fund their activities?

Yes, FINTRAC has observed several instances of IMVE threat actors in Canada using virtual currencies to fund their activities. There is a growing use of cryptocurrency by IMVE threat actors, specifically by cross-border networks and organized groups. These threat actors typically send and receive funds to and from cryptocurrency exchange platforms, which have an obligation to report designated financial transactions to FINTRAC. In some cases, individuals suspected of engaging in IMVE activity used cryptocurrency exchanges and their personal banking accounts to facilitate the flow of funds within the financing network. FINTRAC assessing that the use of cryptocurrency by cross-border networks and organized groups could allow threat actors to raise significantly larger amounts of funds that would otherwise raise suspicions if conducted through regular personal or business banking accounts.